




Department of Energy

Washington, DC 20585

September 14, 2006

MEMORANDUM FOR HEADS OF DEPARTMENTAL ELEMENTS

FROM: THOMAS N. PYKE, JR. 
CHIEF INFORMATION OFFICER

SUBJECT: Transmittal of Department of Energy Chief Information Officer
Guidance CS-6, Plan of Action and Milestones Guidance

Consistent with the goals and processes outlined in the Cyber Security Program Revitalization Plan, I am approving and issuing the attached Guidance, *DOE CIO Guidance CS-6, Plan of Action and Milestones Guidance*.

The Plan of Actions and Milestones (POA&M) process is a management tool for identifying, assessing, prioritizing, and tracking needed corrective actions that mitigate cyber security weaknesses. This process is to be used to ensure appropriate, documented response to every weakness identified by GAO, the Inspector General, the Office of Safety and Security Performance Assurance, the Office of the CIO (OCIO), and by program managers and system owners who conduct reviews of their systems. One set of POA&M corrective actions is developed during the system certification and accreditation process.

This Guidance, which was developed by the OCIO and reviewed by the Cyber Security Working Group, provides a unified and consistent approach to the POA&M process to be addressed in Senior DOE Management Program Cyber Security Plans (PCSPs) and implemented throughout the Department. We will need to work together closely during the next year as we manage the POA&M process so as to mitigate the weaknesses in this process that our Inspector General has just identified. For example, findings are not always being incorporated into POA&Ms, and they are not being addressed in a timely way. We plan to roll out a Department-wide POA&M management process that will give your office and OCIO insight in some detail of the status of all POA&M actions, so we can all ensure this important part of cyber security management is receiving the attention it requires.

I request your help to ensure that this Guidance is promptly and adequately addressed in your organization's PCSP, and implemented throughout the organization. The OCIO, in coordination with the Office of the Inspector General and the Office of Security and Safety Performance Assurance, will assess the implementation of this Guidance in organizational PCSPs as well as implementation at headquarters and in the field. Thank you for your personal attention to ensuring that the content of this new Guidance is integrated into your organization's cyber security program as soon as possible.

Please contact Bill Huntman, Associate CIO for Cyber Security, at 202-586-1090, with any requests, comments, or questions.

Attachment

